AUSA: Kevin M. Mulcahy Telephone: (313) 226-9100
Special Agent: Amy M. Hirina Telephone: (248) 879-6090

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 3622 Lorena Drive, Waterford, MI, 48329 (more fully described in Attachment A)	)	Case No. 2:21-mc-50001 Judge: Lawson, David M. Filed: 01-04-2021

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 2252A(a)(2)	Receipt and distribution of child pornography
18 USC § 2252A(a)(5)(b)	Possession of child pornography

The application is based on these facts:

See attached AFFIDAVIT.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Amy M. Hirina, Special Agent (FBI)
Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Date: January 4, 2021

Judge's signature

City and state: Detroit, Michigan

Hon. Patricia T. Morris, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

In the Matter of the Search of
3622 Lorena Drive
Waterford, MI, 48329

FILED UNDER SEAL

_____/

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Amy Hirina, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Detroit Division, being duly sworn, depose and state as follows:

I. INTRODUCTION

1. I have been employed as a Special Agent of the FBI since 2005, and am currently assigned to the FBI Detroit Division, Oakland County Resident Agency. While employed by the FBI, I have investigated federal criminal violations involving the online sexual exploitation of children. I have gained experience through training at the FBI Academy, post Academy training, and everyday work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I am conducting an investigation related to violations of the following statutes: 18 U.S.C. § 2252A(a)(2) (Receipt and Distribution of Child Pornography) and 18 U.S.C. § 2252A(a)(5)(B) (Possession of Child Pornography) (hereinafter the "TARGET OFFENSES"). Based on the evidence discovered during the course of my investigation, I have probable cause to believe that the evidence related to the TARGET OFFENSES is located within the premises described as 3622 Lorena Drive, Waterford, MI, 48329 (hereinafter the "SUBJECT PREMISES").

4. Consequently, I am submitting this affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES.

5. I am requesting authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of a crime. I am requesting that the search warrant authorize the search of vehicles located at or near the residence which fall under the dominion and control of the person(s) associated with the SUBJECT PREMISES.

6. The search of the vehicles located at or near the residence that are under the dominion and control of persons associated with the SUBJECT PREMISES is to include all internal and external compartments and all containers that may be capable of storing computer media or other repositories associated with the storage of child pornographic materials or their instrumentalities.

7. The statements in this affidavit are based on my investigation of this matter, as well as the receipt of information from other FBI personnel and local law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities related to the TARGET OFFENSES are presently located at the SUBJECT PREMISES.

II. PROBABLE CAUSE

A. The Undercover Operation

8. An FBI Online Covert Employee (OCE) was operating as an adult male on Kik, which is an internet-based messaging application. On approximately September 12, 2020, FBI OCE observed Kik user "bleach678"/display name "Bleach Darim" post a video of an adult female performing oral sex

on a minor female, who appeared to be approximately four years old. The video was posted in the Kik group "ch.ildren"/display name "share and T R A D E."

9. On approximately September 19, 2020, FBI OCE observed the following in the Kik group "ch.ildren"/display name "share and T R A D E:" "Username unavailable Rage bot" posted "There's 50 people here, removing last active members from #ch.ildren," and "If you like to stay in the group indefinitely send one video or link to the admin."

10. On approximately September 20, 2020, FBI OCE observed the following in the Kik group "ch.ildren"/display name "share and T R A D E:" Kik user "bleach678"/display name "Bleach Darim" posted a video of a nude female approximately ten years old touching her genitals. The two videos posted by Kik user "bleach678"/display name "Bleach Darim" meet the federal definition of child pornography.

B. Identifying James and Heather Kessler (SUBJECT PERSONS)

11. On or about September 22, 2020, MediaLab responded to a subpoena seeking information for Kik account "bleach678" with the following information:

First Name: Bleach
Last Name: Darim
Email Address: bleach678@gmail.com

IP Addresses:
2020/09/15, 13:00:36 UTC, 24.127.163.109, remote port 52664
2020/09/06, 15:35:29 UTC, 174.230.36.147, remote port 9392

12. An open source search revealed IP address 24.127.163.109 belonged to Comcast.

13. On or about September 24, 2020, Comcast responded to a subpoena seeking information on IP address 24.127.163.109, port 52664 assigned on 2020/09/15 at 13:00:36 UTC with the following information:

Subscriber Name: James Kessler
Service Address: 3622 Lorena Drive, Waterford, MI 48329 (SUBJECT PREMISES)
Telephone: 248-310-9518

14. An open source search revealed IP address 174.230.36.147 was assigned to Verizon Wireless.

15. On or about September 30, 2020, Verizon Wireless responded to a subpoena seeking information on IP address 174.230.36.147, port 9392 assigned on 2020/09/06 at 15:35:29 UTC with the following information:

Subscriber Name: Heather Cole
Service Address: 3622 Lorena Drive, Waterford, MI 48329 (SUBJECT PREMISES)
Telephone: 248-310-9518

16. A search of the Michigan Secretary of State database revealed the following residents registered to 3622 Lorena Drive, Waterford, MI 48329 (SUBJECT PREMISES): James Kessler, DOB 11/XX/1986, and Heather Kessler (nee Cole), DOB 10/XX/1990.

III. CHARACTERISTICS OF PORNOGRAPHY PARTICIPANTS

17. In addition to participating in child exploitation investigations, your affiant has discussed the aspects of computers and their relationship with child pornography offenses with others. Based upon my knowledge, experience, and communications with other individuals involved in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography.

18. Based on my training and experience, and the training and experience of other agents, I believe that a resident residing at or visiting the SUBJECT PREMISES is a collector of child pornography. I base this conclusion on the following facts:

    a. Individuals who receive and collect child pornography may receive sexual gratification, stimulation, and satisfaction viewing children engaged in sexual activity, in sexually suggestive poses such as in person, in photographs, other visual media, or from

literature describing such activity. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification;

b. Individuals who receive and collect child pornography do so in a variety of media, including, but not limited to, digital images and videos of child pornography;

c. Individuals who receive and collect child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Maintaining these collections in a digital or electronic format in a safe, secure and private environment, such as a computer in a private residence, allows the collectors the opportunity to safely maintain their collections for many years and enable the collector to frequently view the collection, which is valued highly. Based on the evidence obtained in this investigation, the files of child pornography accessed, possessed, and potentially offered for others to download by the computer or other electronic devices located at the SUBJECT PREMISES, are being stored at a private residence; and,

d. Child pornography collectors may also correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit materials; and often maintain lists of

names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Based on the evidence obtained in this investigation, an individual likely used an electronic device and the internet to request child pornography files.

19. Based on my training and experience and my conversations with other investigators, child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes, at their private residence, for many years. The nature of the materials, their attraction to the materials, and the risk involved with receiving, downloading, and possessing such materials, motivates collectors to keep their child pornography collection within their possession and control wherever they go. Because collectors of child pornography place an extremely high value on their collection, they will take their collection with them if they move from one location to another or else keep it in a secure location nearby.

20. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

IV. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

21. In my training and experience, I know that cellular phones ("smart phones") contain software and hardware that are the same, if not more sophisticated, than a typical home computer. The term "computer," "hard drive," and "computer media," as used in this affidavit, also refers to cellular "smart" phones.

22. I also know that "smart phones" often allow for cloud-based storage, and many users back up their phones on their home computers. Information contained in a phone that is connected to a desktop or laptop computer, can easily transfer onto other media.

23. A computer's ability to store images in digital form makes a computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

24. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

25. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, iCloud, and Hotmail, and social media applications such as Kik, Telegram and Snapchat among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer, even if the user is accessing the information on their cellular "smart phone." Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

26. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP

client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or

weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and,

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been

used to create the data (whether stored on hard drives or on external media).

29. In addition, there is probable cause to believe that the computer and its storage devices are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

30. Affiant knows from training and experience that even if the files were deleted by a user, they still may be recoverable by a trained computer forensic examiner. Specifically, when a user deletes a file, it goes into a "trash" folder. When the user directs the computer to "empty" the trash folder the contents of the folder, including the deleted file, disappear. However, the file has not left the computer and under normal circumstances, is recoverable by computer experts until it's overwritten because there is no longer unused space in the computer's hard drive. How soon a file will be overwritten depends on a number of factors: whether the user is computer savvy and has installed a program that accelerates the normal overwriting of deleted data, how often new files are saved to his hard drive, the capacity of the hard drive, and how the computer's file system allocates new files. Trained certified computer forensic examiners

routinely extract incriminating deleted files from hard drives, usually without difficulty.[1]

31. Since a deleted file is not overwritten all at once, it may be possible to reconstruct it from the bits of data composing it (called "slack data"), which are still retrievable because they have not yet been overwritten even if overwriting has begun. Before a file is deleted, the file system marks it as unavailable to be overwritten. Once it is deleted, its data are no longer protected against being overwritten, but the file system won't necessarily overwrite it all at once, and if it's only partially overwritten computer experts can recover the portion of the data that has not been overwritten, or at least can match it to images they obtained from, for example, a website, to verify that the images were once in the computer's hard drive and thus had been possessed.[2] Although a savvy computer user can direct his computer to ensure quick (even instantaneous) overwriting, the default settings on standard operating systems do not do this.[3]

[1] *United States v. Seiver*, 692 F.3d 774, 776-77 (7th Cir. 2012).
[2] See Michele C.S. Lange & Kristin M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know Now* 235 (2d ed. 2009).
[3] *Seiver*, 692 F.3d 776-77.

32. It is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which specific expert possesses sufficient specialized skills to best obtain the evidence and subsequently analyze it. No matter which method is used, the data analysis protocols that will be utilized are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Upon approval and execution of the search warrant, in appropriate circumstances, a forensic image (also known as a bit-stream image), which is an exact physical copy of the seized electronic evidence, will be created so that their contents could be examined at a field office or computer laboratory and/or other locations following completion of the on-site search.

33. The search of computers, hard drives, and other seized electronic media will include a complete search of the entire piece of seized electronic evidence. A computer forensic examiner cannot rely on the name of a file to exclude or confirm the existence of child pornography within that file. Individuals will intentionally mislabel directory structures, folder names, and filenames to hide the presence of child pornography. In other cases, an individual may not attempt to hide the child pornography but utilize a unique naming convention or organizational methodology which may

inadvertently hide the presence of child pornography. In order to perform a comprehensive forensic examination, a computer forensic examiner must conduct an all-inclusive examination of every bit (or binary digit) on the particular electronic storage device.

34. Moreover, hard drives and other pieces of electronic media have unallocated space which might contain deleted files, records, relevant e-mails, other communications, and search terms related to the possession, receipt, and distribution of child pornography. Thus, without looking at the entirety of the electronic media for evidence related to child pornography, the investigator may not find evidence relevant to the criminal investigation.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

35. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital

storage device(s) to help identify any other relevant evidence and/or potential victim(s);

b. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. surveying various file directories and the individual files they contain;

e. opening files in order to determine their contents;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or,

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

A. Use of Biometric Features to Unlock Electronic Devices

36. The warrant I am applying for would permit law enforcement to compel James Kessler and/or Heather Kessler to unlock a device subject to seizure pursuant to this warrant that is in his/her possession or for which law enforcement otherwise has a reasonable basis to believe is used by him/her using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often

referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices

produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was

last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

37. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and the device is in James Kessler and/or Heather Kessler's possession or law enforcement otherwise has a reasonable basis to believe is used by James Kessler and/or Heather Kessler, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of James Kessler and/or Heather Kessler to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of James Kessler and/or Heather Kessler and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of James Kessler and/or Heather Kessler and activate the iris recognition feature, for the

purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

VII. CONCLUSION

38. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that an individual(s) who resides at the SUBJECT PREMISES, described above, has violated 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography).

39. Additionally, there is probable cause to believe that evidence of the commission of TARGET OFFENSES is located at the SUBJECT PREMISES described above and more fully in Attachment A. The evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

40. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,

Amy M. Hirina, Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence
and/or by reliable electronic means.

HON. PATRICIA T. MORRIS
UNITED STATES MAGISTRATE JUDGE

Date: January 4, 2021

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as **3622 Lorena Drive, Waterford, Michigan 48329** (SUBJECT PREMISES), is identified as follows: The residence is a light colored brick and siding, single family residence. The residence is marked with "3622" above the garage. The residence is located on Lorena Drive between Watkins Lake Road and Pine Orchard Drive

The SUBJECT PREMISES includes any vehicles located on the premises and under the control of James Kessler and/or Heather Kessler.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:

    a. Any computer, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices);

    b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and

    c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents and records regarding the ownership and/or possession of the SUBJECT PREMISES.

6. During the course of the search, photographs of the SUBJECT PREMISES and any vehicles may also be taken to record the condition thereof and/or the location of items therein.

AUSA: Kevin M. Mulcahy Telephone: (313) 226-9100
Special Agent: Amy M. Hirina Telephone: (248) 879-6090

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 3622 Lorena Drive, Waterford, MI, 48329 (more fully described in Attachment A)	)	Case No. 2:21-mc-50001 Judge: Lawson, David M. Filed: 01-04-2021

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Michigan.
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

YOU ARE COMMANDED to execute this warrant on or before January 18, 2021 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: January 4, 2021 10:44 am

Judge's signature

City and state: Detroit, Michigan

Hon. Patricia T. Morris, U. S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title